H10－認証･公証WG

企業間電子商取引における
認証・公証適用の考え方

Version　０．５

平成１１年３月

電子商取引実証推進協議会
認証・公証WG

はじめに

ＥＣＯＭではフェーズ１で主として企業対消費者間の電子商取引（以下、ＢtoＣという）を念頭において、そこで必要になる認証（authentication）について検討し、その結果を幾つかのガイドライン、評価基準等として公表してきた。

一方、従来から専用線の利用を前提として実現されてきた企業間電子商取引(以下、ＢtoＢという)に関しても、インターネットに代表されるオープンネットワークの利用構想が具体的に見えてきた。オープンネットワークでは成りすまし、盗聴、改竄等の商取引の安全性を脅かす脅威の大きさは専用線網の比ではなく、これらに対する具体的な対策が求められている。認証･公証機能は正にこれらの脅威に対抗するものであるが、ＢtoＢの認証・公証はＢtoＣのそれと全く異なるものではなく、むしろ延長線上にあるものなので、ＥＣＯＭの認証・公証ＷＧではフェーズ２の主要なテーマとして、これに取り組んできた。

公共調達等のように取引当事者の一方が政府・自治体であるケースも、取引の側面から見ると、企業同士の間での取引と本質的には同じであり、企業間取引の一環として考えることにする。（以下ではこのケースをＢtoＧという。）

ＢtoＢ／ＢtoＧにおいて要求される認証機能は基本的にはＢtoＣの場合と同じであるが、ＢtoＢ／ＢtoＧでは相手企業が取引相手としての信用を備えているかの確認につなげ得るものであることが要求される。また企業としての認証に加えて、実際の取引を行う担当者の当該取引に関する権限の確認も要求される場合がある。

従来、企業間で取引を始める際には商業登記による相手企業の実在確認が使われるケースが多かった。法務省では電子商取引においても商業登記の同様の使い方ができるように、商業登記に基づく電子認証サービスを具体化しつつある。ここではこのような公的認証サービスとの関連についても、その位置づけを明らかにしている。

オープンネットワークを利用する際に必要な認証機能として、（イ）相手の確認、（ロ）通信内容が発信者の意思を反映したものであることの確認、（ハ）通信途上で改竄されていないことの確認が挙げられる。

この内で（イ）に関しては、パスワードのような秘密共有に基づく方式、公開鍵暗号を利用するデジタル署名に基づく方式、指紋等のバイオメトリクスに基づく方式が考え得るが、以下の理由から認証局を利用したデジタル署名方式が現状では最も適している。

パスワード方式は取引関係が１対ｎの企業間に限定される場合には、通信途上での盗聴・再利用に対して適切な対策を施せば、充分使える方式であるが、取引形態がｎ対mの企業間のケースでは運用しにくい。バイオメトリクス方式は企業という非自然人に対して直接適用できない本質に加えて、パスワード方式と同様にｎ対m環境では運用しにくい性質がある。また本質的に反復性を持つ情報を用いるので通信途上での盗聴･再利用に対抗する対策が必要であるのに加えて、ネットワークを介してのライブテストがやりにくい側面もあり、ネットワークを介した相手確認には適用しにくい面がある。デジタル署名方式は１対ｎ環境では認証書を必要としないが、認証書を併用すればｎ対m環境にも対応できる。

（ロ）に関しては現時点における確立した技術としてデジタル署名以外の解が見えていない。また（ハ）に関しては、共通鍵暗号を用いるＭＡＣ（Message Authentication Code）のような方式も適用できるが、勿論デジタル署名も改竄検出機能を備えている。

これらの考察から本ドキュメントでは認証に関しては認証書を用いるデジタル署名を用いる方式に絞って適用の考え方をまとめた。それ以外の方式に適用性がないと考えている訳ではなく、それらの方式は既に長い歴史があってその利用に際しての考え方が良く知られているのに対して、認証書を用いるデジタル署名は比較的新しい技術で注目されていること及び適用の考え方を早急に出すことが要請されていることを勘案した結果である。

公証に関しては、紙をベースとした世界では従来から公証人制度が用いられてきた。法務省ではこの制度に基づく電子公証を具体的に検討しており、その実施も計画されているようであるが、ここではそれよりも広いスコープで公証を捉えることにして、私的公証の考え方を述べている。因みに公証とは「公に証明する」という意味であって、「公が証明する」のではないので、私的公証という表現は一見奇異に感じるが、矛盾した考え方ではない。

企業間取引における公証の本質は、取引に関する事実に第三者対抗要件を確立させることにあると考えており、第三者としてあらかじめ契約で設定された企業グループの構成員を想定する場合には、その企業グループ内で構成員の合意に基づく公証機能を考えることが可能になる。これを私的公証と呼ぶ。この場合には企業グループの構成員以外の第三者に対しての対抗要件は具備し得ず、そのような相手とのトラブルに対しては、事前にそのような場合を想定して公的公証を利用するか、トラブル発生後の裁判に委ねることになる。勿論、企業グループ内に閉じたケースを想定した場合であっても公的公証を利用することも考え得る。どの考え方に立つかは、運用面、コスト面からの考察によるべきである。

企業間取引において要求される公証機能は、取引当事者、取引時点、取引内容等の取引に関する事実を公証機関が証明する形で実現される。私的公証と公的公証との違いは、この公証機関の第三者性・中立性が認められる範囲による。即ち、企業グループを形成するための契約によって、この第三者性・中立性が担保される場合が私的公証であり、その公証機関としての有効性はその企業グループ内に閉じるのに対して、公的な制度によってこれが担保されるのが公的公証であって、その公証機関としての有効性はあらかじめ契約を交わしておくことのできない相手にも及ぶ。

このドキュメントはＢtoＢ／ＢtoＧのアプリケーション実現に際して、認証・公証をどのように適用してゆくかのためのガイドライン策定に当たり、企業間取引における認証･公証の枠組みをまとめたものであって、アプリケーションの捉えかた、認証の考え方、公証の考え方、それぞれの情報の流れと関与するプレーヤを述べたものである。今回は現時点における考え方をまとめた中間版をレビューして頂くためのたたき台として公開するものであり、関係各位からのコメントを取り入れて、現実のアプリケーションに即したものに修正していくための一つのステップである。

なおコメントは下記宛にくださいますようお願い致します。

電子商取引実証推進協議会(ECOM)
認証・公証ワーキンググループ／企業認証・公証サブワーキンググループ
〒135-8073 東京都江東区青海 2-45 タイム 24 ビル 10 階
TEL：(03)5531-0061　FAX：(03)5531-0068
E-mail：an2jimu@ecom.or.jp(認証・公証ワーキンググループ事務局)
http://www.ecom.or.jp

目次

第1章　認証局を利用した企業認証適用の考え方

1.1.　アプリケーションモデル

企業間の取引きは様々な形態で行われている。またその中で行われている取引きにおいて各プロセスの果たす役割も局面により異なる。ここでは電子商取引においてそれらの役割や機能を実現するために、アプリケーションに要求される機能や、想定できるモデルについて説明する。

1.1.1.　　取引モデル

本節ではこの章で取り扱う「取引」の定義を行い、取引きにおける参加者やその機能・役割を取引プロセス毎に整理することで取引きに必要な要件を明らかにするとともに、取引きにおける形態を分類し取引きのモデル化を行う。

(1)　　取引参加者とその機能・役割

「取引」とは個人－個人間、個人－企業間、企業－企業間など様々な形で行われる売買行為を指すが、本章では企業―企業間の取引きを主として取り扱う。

企業間で行われる取引きの参加者は、商品となるサービスや物品の提供をする企業と対価を払いそれらを享受する企業に大別することができるが、それらが取引きのプロセスとして行う契約、受発注、決済などの行為は様々な形式で行われ一様ではない。

ここでは一般的な取引きの流れを例示し、その場合の各参加者の機能や役割を整理するが、必ずしも現実の取引きで、それらを規定することを意味するものではない。

- 取引きの流れ（例）
  A 社：商品となるサービスや物品の提供をする企業
  B 社：対価を払い商品を享受する企業

表 1-1 取引きの流れ（例）

取引きの流れ		A 社の機能・役割	B 社の機能・役割	取交わされる書類等
包括的な契約		B 社の 存在証明 信用調査 取引能力調査	A 社の 存在証明 信用調査 取引能力調査	基本契約書 商業登記簿謄本 代表者印鑑証明 財務諸表 企業情報など
商品の受発注	個別契約	契約内容の提示 本契約に対する 取引能力調査	契約内容の確認 本契約に対する 取引資格証明	個別契約書 資格証明書 財務諸表 企業情報など
	注文書の授受	注文内容の提示	注文内容の確認	注文書 注文請書など
商品の納入／検収		商品の納入	商品の検収	納品書 受領書 検収報告書など
決済		取引代金の請求 取引代金の領収	取引代金の振込	請求書 領収書など

上記の例で示されるように取引きの流れにおいては、その各プロセスにおいて何らかの方法で認証という行為（ここでは「取交わされる書類等」によって）が行われている。企業間の取引きで、その基礎となる認証は相手企業の存在証明である。その他、相手企業の知名度、業界の安定度などから信用調査、取引能力調査などの必要性が考えられるが、その方法は取引内容や取引きの連続性（継続的な取引きか、非継続的な取引きか）、取引金額の大小などにより異なることが考えられる。

また、前記のような証明、調査を行った場合においても取引き上の契約が必ず履行されるとは限らないことから紛争が起きた場合、迅速に解決するために公正証書や確定日付などを使用した取引事実の証拠力を強める手段が必要な場合も考えられる。

(2)　取引形態

企業間で行われる取引きの形態は、その取引きの参加方法によって分類すると以下のように大別することができる。

- 契約型取引形態…取引きに参加する時点で契約を交わす必要がある取引形態
- 公募型取引形態…取引きに参加する時点では特に契約を交わす必要がない取引形態

①　契約型取引形態

契約型とは企業間で取引きを行う際、その取引きに参加する時点または事前に企業間にお

いてなんらかの契約を交わす取引形態である。企業は互いに取引相手となる企業を選別し、合意の基で取引きを行う。

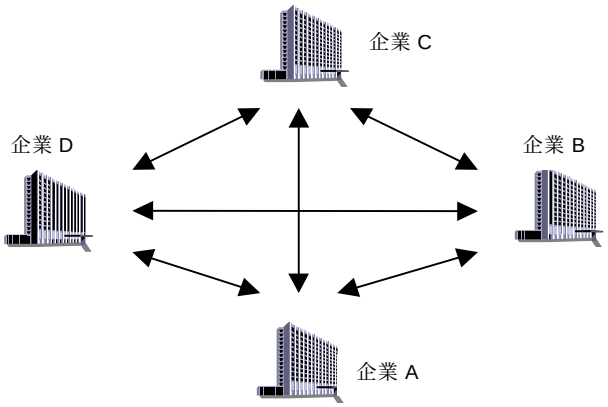

図 1-1 契約型取引形態

② 公募型取引形態

公募型とは企業間で取引きを行う際、その取引きに参加する時点では特に契約を行わず取引きに参加する取引形態である。企業間には募集者と応募者のような関係があり、応募者は募集者の提示する応募条件を満たしていれば自由に参加することができる。

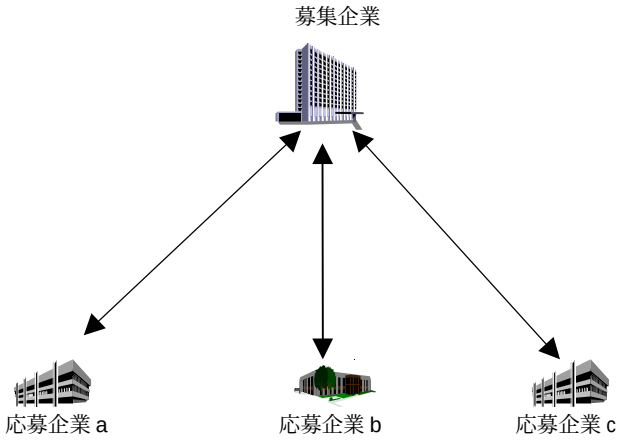

図 1-2 公募型取引形態

1.1.2. 認証実現の形態

ネットワークを介した電子商取引を行う場合も、現実の取引きにおいて行われる取引プロセスを同様に行うために、存在証明や信用調査、取引能力調査などを行う必要が考えられる。また、電子商取引では通信相手の本人確認や通信内容の真正性など、ネットワークならではのセキュリティ機能も必要になる。

これらの機能を実現する 1 つの方法として「公開鍵方式による認証局を利用した企業認証」が考えられる。この形態では、認証局が認証書を発行・管理することになる。ここで認証書とは少なくとも利用者の情報と公開鍵（ビット列）の情報を含むデジタル文書に認証局

のデジタル署名を付したものを言う。
「公開鍵方式による認証局を利用した企業認証」では取引きを行うとき、認証局により発行された認証書を、取引情報とともに相手企業に対し送信する。相手企業は認証書により成りすまし防止やメッセージ改竄防止等のネットワークセキュリティーを確保できるとともに、認証局による企業の存在証明等の認証を行うことができる。
本節では、電子商取引における認証のモデルについて述べる。

(1) 認証の対象と認証の機能とその利用目的

企業認証の認証対象（エンティティ）としては、次の３つが考えられる。

- 代表者
- 権限のある個人
- 企業

これらのエンティティとしてどれを採用するかは、取引きの環境・条件・当事者間の合意等によって定まる。
また、認証の機能レベルには、企業認証の有用性によって以下のようなレベルが考えられる。

(1) 本人性・実在性を証明する
(2) (1)+権限・資格を証明する
(3) (2)+与信

本書では、(1)及び(2)のレベルを扱う。

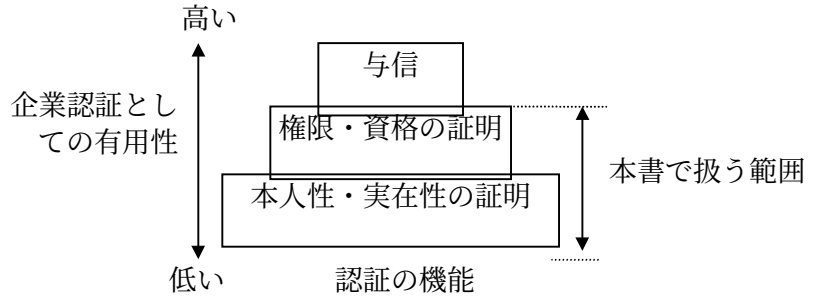

図 1-3 企業認証のレベルと本書の対象

(2) 各取引モデルにおける認証の利用形態

前述の各取引モデル（１．１．１）における認証の利用形態を以下に示す。

① 契約型取引形態における認証

契約関係にある企業の合意の下に設立された認証局や、契約の中心となる企業が運営する認証局によって発行される、参加企業の存在を証明する認証書や、権限もしくは資格を証明する認証書を利用して、取引きを行う。

A. 認証書の発行形態

認証書の発行形態には、契約企業グループ内に設立された認証局が発行する形態と、契約の中心となる企業が運営する認証局が発行する形態の２種類がある。

a．契約企業グループ内に設立された認証局が発行する形態

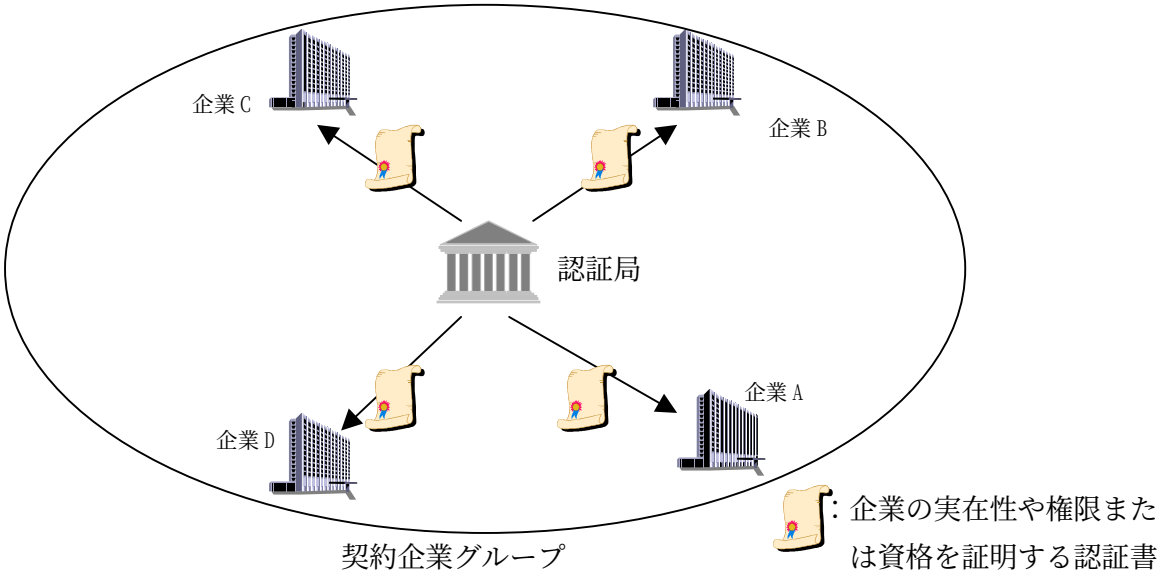

図 1-4 契約企業グループ内に設立された認証局が発行する形態

b．契約の中心となる企業が運営する認証局が発行する形態

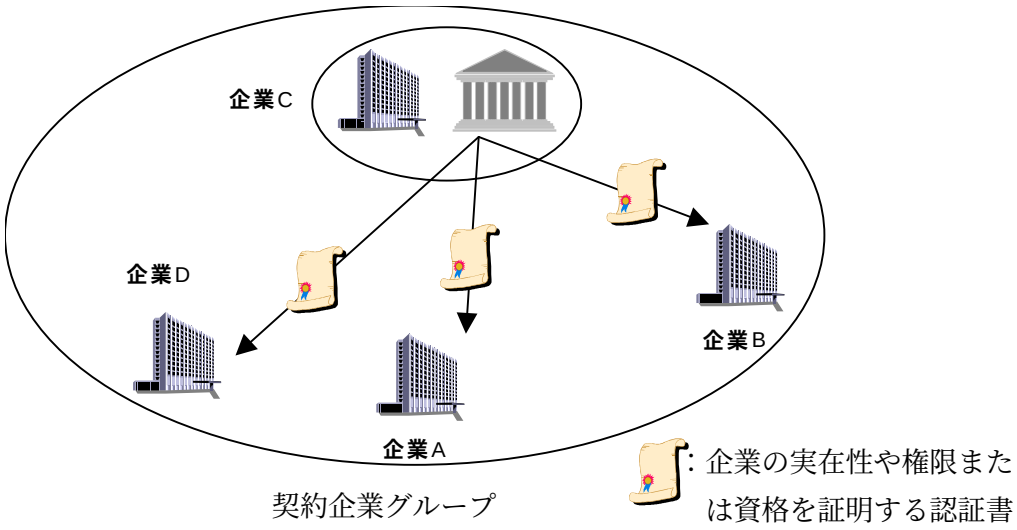

図 1-5 契約の中心となる企業が運営する認証局が発行する形態

B．認証書の利用形態

前述の認証書の発行形態に関わらず、各企業は取引き毎に、取引相手と相互に認証書の交換を行う。認証書の提示を受けた企業は、提示された認証書の有効性を、認証局に問い合わせて確認する。

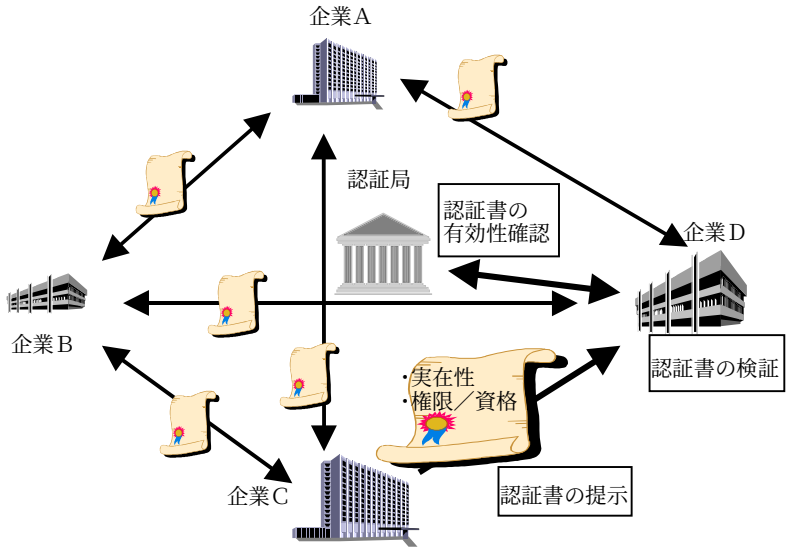

図 1-6 契約型取引における認証書の利用形態

② 公募型取引形態における認証の利用形態

すべての公募参加企業が信頼できる認証局によって発行された、公募参加企業の存在性を証明する認証書を利用して、公募に参加する。発行された認証書は、募集企業と応募企業の間のみで交換される。このとき、応募企業から募集企業に対して提示される認証書を発行する認証局は、募集企業の提示する応募要件として指定されることが考えられる。

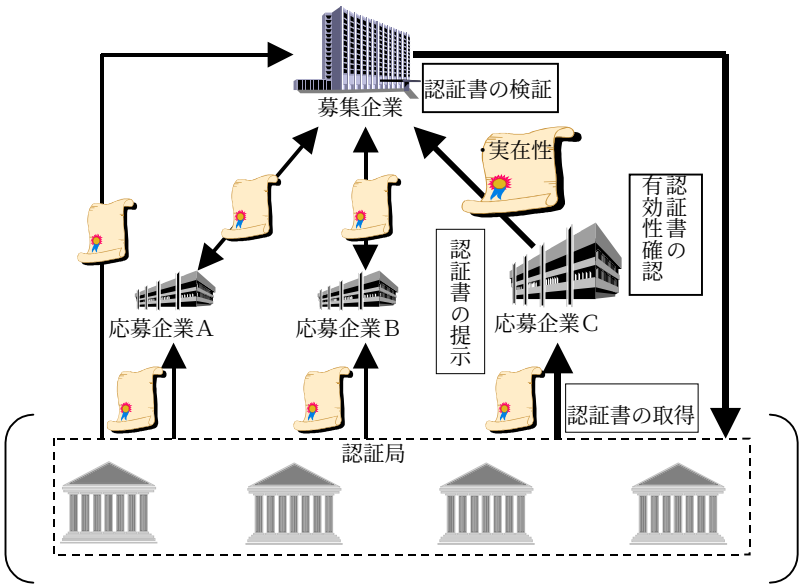

図 1-7 公募型取引形態における認証の利用形態

なお、図では略されているが、応募企業も募集企業の認証書の有効性を確認する。

(3)　認証局の構成

認証書の発行対象となる企業間電子商取引参加企業数、企業の地域的広がり、認証検証等の処理負荷、異なる取引きグループとの相互認証等の事情に応じて、認証局が以下の様な構成を取る事がある。

- 単一認証局モデル　：　単一の認証局が存在するもの
- 階層型認証局モデル　：　認証局間に階層関係があるもの
- 水平型認証局モデル　：　認証局間が対等であるもの

①　単一認証局モデル

認証局構成の基本モデルであり、全ての取引参加企業は唯一の認証局から認証書の発行を受ける。

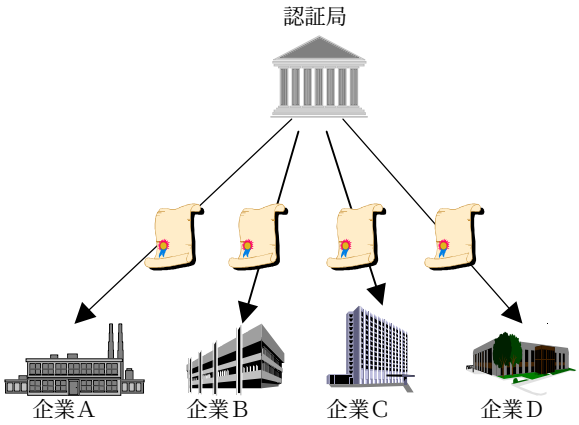

図 1-8 単一認証局モデル

②　階層型認証局モデル

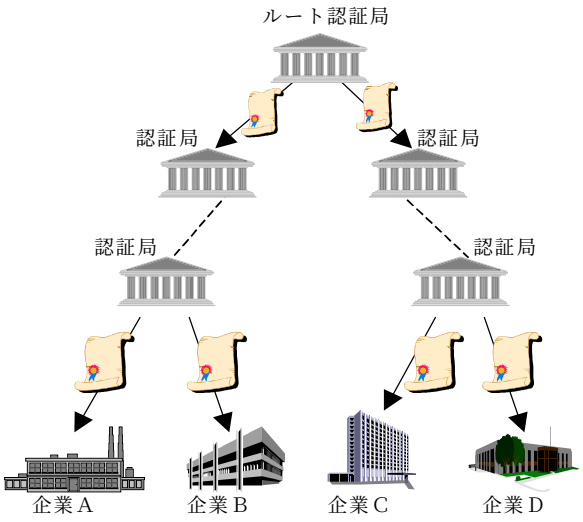

図 1-9 階層型認証局モデル

この構成は、参加企業数が多数であったり、認証局の負荷分散・危険分散等の理由で同一ポリシーを持つ複数の組織が認証局を運営する形態である。

このモデルでは、複数の認証局が、階層構造により構成されており、最下位ノードに位置する認証局は、取引参加企業に対して認証書を発行する。一方、最下位ノード以外に位置する認証局は、下位の認証局に対して認証書を発行する。なお、上位認証局が下位認証局に認証書を発行する場合には、設備や運用体制、ポリシー等に関して厳密な審査が必要となる。

③　水平型認証局モデル

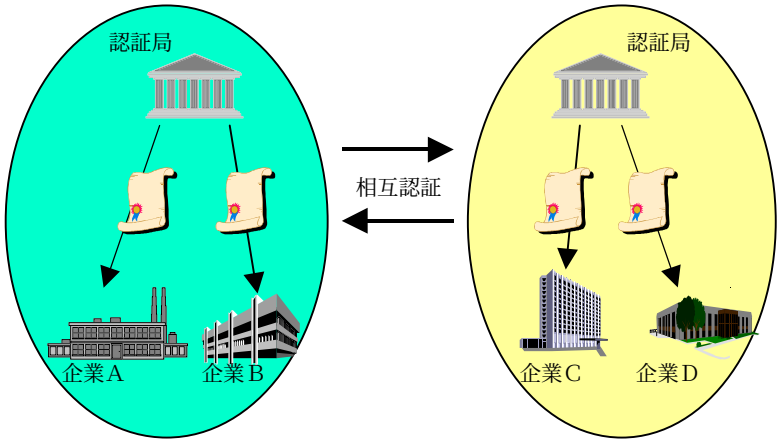

図 1-10　水平型認証局モデル

このモデルでは、複数の認証局が、互いに対等な関係を持って存在している。

このため、他の認証局によって発行された認証書を検証する（相互認証）仕組みを提供する必要がある。相互認証の仕組みとしては、

- 自分の認証書を発行した認証局に、相手の認証書の有効性を問い合わせる
- 相手の認証書を発行した認証局に有効性を問い合わせる
- 仮想的なルート認証局を作成する

など、いくつかの方法が考えられる。

実際には、水平型認証局モデルは、複数の階層型認証局モデルから構成される場合が多い。

1.2.　認証ポリシーの策定

本節では、「公開鍵方式による認証局を利用した企業認証」を適用するに当たり、先ず必要となる認証ポリシーとその策定についての概要を述べる。

1.2.1.　　認証ポリシーとは

認証ポリシーは、特定の認証書の適切な利用目的に対して、認証書取得者及び認証書検証者（併せて利用者と呼ぶ）双方に理解できる形式により、認証局が認証書利用者に提示するものであり、当該認証ドメインに参加しようとする利用者（企業など）は、認証ドメイン内のポリシー制定主体が設定・表明した認証ポリシーを利用する。なお認証ドメインとは認証局から発行される認証書を使用する取引参加企業から構成される電子商取引業務を実現するシステム全体を示し、同一の認証ポリシーを共有する法人あるいはその他の団体の集合を指す。

1.2.2.　認証ポリシーの表現方法

認証ポリシーを表現する手段として、Ｘ．５０９ Ｖ３認証書の認証書ポリシーフィールドを使用するもの、ＣＰＳ（Certification Practice Statements）を作成するものなどがあり、通常この両者が設定される。認証書ポリシーフィールドはX．５０９認証書中にあり、利用者（企業など）が確認できるようになっている。あるポリシー制定主体はこのフィールドを利用して、簡単な声明文を掲載することは可能である。しかしながら、認証書の長さの問題もあり、ポリシーのオブジェクトＩＤ（ポリシーＯＩＤ）のみを設定し、ポリシーＵＲＬあるいはポリシーＥ－ｍａｉｌというフィールドに詳細なポリシーをポイントするアドレスを掲載することにより、利用者（企業など）が参照可能にすることも可能である。現在、この認証書ポリシーとＣＰＳの法的拘束力の優先的順序性は定義されていない。従って、認証書ポリシーが認証書の適用分野・クラスを示す認証ドメインの一般的特性を幅広く声明するもの、また、ＣＰＳが当該認証ドメインのビジネスの実践について、その責任範囲について詳細に記述したものであると考えるなら、認証書ポリシーとＣＰＳには密接な関係があり、相互に補完するものと考えるべきである。

さらに、この両者は認証ポリシーを共有する認証ドメイン内でビジネスの実践に先立って行われる契約で関係付けることも可能である。例えば、ビジネス契約の付帯条項あるいは付帯文書として参照させる方法であり、もし異なる表現があったなら、どちらを優先させるかを規定することも可能であろう。

一方、異なるＣＰＳを持っている認証ドメイン間で同一の認証書ポリシーを使用したり、異なる認証書ポリシーを持っている認証ドメインが同一のＣＰＳを使用することは有り得る。これは異なる認証ドメイン間で相互認証をするときに有効であり、ＣＰＳを作り直したり、認証書を発効し直す労力を避けるのに役立つ。しかし、このときでも相互の認証ドメイン間の契約書の見直しは必要である。

ＩＥＴＦでは、認証書ポリシーやＣＰＳを制定する人が、相互認証あるいは認証ポリシーの検証を目的に、認証ポリシーの規定形式を以下のような標準の型として提供しているので、実際の認証ポリシー策定では、これを利用することも可能である。

- はじめに
- 一般条項
- 知的所有権
- 運用上のリクワイアメント
- 物理的、手続き上、人事上のセキュリティ管理
- 技術的なセキュリティ管理
- 認証書とＣＲＬの概要
- 仕様の管理

オブジェクトＩＤ（ポリシーＯＩＤ）を利用する方式は、まだ利用環境等が十分でない等の課題があるため、本節ではＣＰＳを利用する形態を想定する。

1.2.3.　認証ポリシーの形成過程

契約型の取引形態を前提とした場合は、基本的には表 １－２のような過程で認証ポリシーは策定されると考えられる。

表 1-2 一般的認証ポリシー策定の過程

#	ﾌﾟﾛｾｽ	内容	担当
1	利用目的の検証	認証局の利用目的の策定 （基本契約条項、業務トランザクションの形式などは、ここで決定され、認証ポリシー制定主体に引き継がれる）	・認証ドメイン代表者[＊1] ・認証ドメイン代表企業 ・国家（法務省など）
2	認証ポリシー制定主体確定	認証ポリシー制定主体の決定	同上
3	ＰＫＩ適用検討[＊3]	業務トランザクションへのＰＫＩの適応検討	認証ポリシー制定主体[＊2]
4	認証構造の決定	当該認証ドメインへの参加者、認証局、ポリシー制定主体間の義務と責任範囲の確定	認証ポリシー制定主体
5	認証ポリシー制定	ＣＰＳの作成	認証ポリシー制定主体
6	基本業務計画との適合性検証	基本契約条項などとの整合性の確認とフィードバック	認証ポリシー制定主体
7	参加者、利用者への開示	参加者（企業）、利用者（企業）に認証ポリシーを開示	認証ポリシー制定主体
8	ビジネスの実施	ＰＫＩを利用し、実際のビジネスを実施	認証ポリシー制定主体
9	認証ポリシー改定	ビジネスを実施した結果のフィードバック	認証ポリシー制定主体

＊ １：認証ポリシーを承認する主体であり、ポリシー承認局と位置付けることも可能。
＊ ２：認証ポリシーを作成し、施行する主体であり、ポリシー認証局と位置付けることも可能。また、認証ドメイン代表者などがそのまま認証ポリシー制定主体を兼ねるケースも考えられる。
＊ ３：ビジネスの要件上、公開鍵認証書を使用した認証システムが必要か、またビジネス実施上効果が期待できるか、対費用効果の評価など実施

しかしながら、次に示すようなケースも考えられる。

ある組織は現在行われている郵便処理を認証を行わない単純な電子メールに変更する計画を立案し、また、ある組織は新規に企業間の受発注システムをインターネット上で行うという計画を立案する。その目的は業務の効率化であったり、秘匿性の確保であったりするが、これらのビジネス要件を満足させるため、計画立案者はこのビジネスへの参加者とその役割を決める必要がある。この計画立案者は通常ビジネス責任者である（企業間の場合、責任企業）。しかし、前者のメール処理では、認証処理を行っていないため、後日には参加者からの認証への要求が高まってくるだろう。この場合、参加者の役割と責務などについての認証ポリシーはビジネスをしながら、充実されていくことになる。

後者の受発注システムでは、高額の金銭移動が有り得るということから、当初より参加者の役割、責務については厳密に規定されるはずである。

要するに認証ポリシーの形成は、ビジネス開始後に参加してくるエンドエンティティからの意見を取り込み、実体に沿う形に成長していくケースと、最初に参加要件などを厳密に規定し、その後はほとんど変更されないケースがあるだろう。

このように、認証ポリシーの形成では必ずしも表１－２の過程を経由するとはかぎらないが、表１－２中の＃４、５の認証構造の決定、認証ポリシー制定に重点を置くか、認証ポリ

シー改定に重点を置くかの違いと考えれば、多くのパタンへ適用ができよう。

なお公募型の取引形態を前提とする場合のポリシー形成過程は、表１－２のプロセスから必要な手続きを選択して、目的に応じた形成過程を形作ってゆくものと考えられる。

1.2.4. 認証の ワーク フロー

認証のワークフローを検討するに当たり、まず認証に係わる登場者間で行われる手続きや情報を明らかにする必要がある。その上で、それらの手続きがどのような処理形態で行われるかを記述する。

(1) 認証局、被認証者、認証書検証者間の手続と交換する情報

企業認証において認証の機能を実現するための認証局、被認証者、認証書検証者の間で行われる手続きはそれぞれ以下のようになる。

①　認証局、被認証者間の手続きと交換する情報

A. 認証書の発行

認証機能を実現するために被認証者に対し認証局より認証書を発行する。認証書を発行するための手続きとして次のような手続きが考えられる。

- 認証書の申請
  被認証者は認証の機能を実現するために、認証局に対し認証書の申請を行う。申請を行う際、被認証者は審査する上で必要となる情報や被認証者の公開鍵などを認証局に提示する。
- 認証書の作成
  認証局は被認証者より提示された情報を基に審査を行い、認証書の作成を行う。
- 認証書の受渡
  認証局によって作成された認証書を被認証者に受け渡す。

B. 認証書の更新

認証書の有効期限到来に伴い、認証局は被認証者の依頼に基づき認証書の更新を行う。認証書の更新を行うための手続きとして次のような手続きが考えられる。

- 認証書の発行と同様の審査、手続き（申請／作成／受渡）が必要になるが、簡便な方法を取ることも考えられる。

C. 認証書の失効

認証書の有効期限内において、秘密鍵の漏洩や消失などの事故が起きた場合、被認証者は認証局に対し認証書の失効の申請を行う。また、被認証者による契約違反等があった場合は認証局による強制的な失効を行う場合も考えられる。認証書の失効手続きとして以下の手続きが考えられる。

- 認証書の失効申請
  被認証者の理由により認証書の失効を行うとき、認証局に対し申請を行う。申請を行う際には申請者が認証書の所有者であることを確認できる情報が必要である。
- 認証書の失効
  認証局は被認証者の申請、または強制的に認証機能を無効化させるため認証書を失効させる。被認証者の申請の場合、本人の確認が必要となる。

D．認証書の一時失効

被認証社の理由により認証機能を一時的に無効化させる場合、被認証者は認証局に対し認証書の一時失効のための申請を行う。また、認証書の失効と同様に認証局による強制的な一時失効も考えられる。認証書の一時失効については失効と同様の手続きを行う。

②　被認証者、認証書検証者間の手続きと交換する情報

A．認証書の送受信

認証書検証者は被認証者の認証書を受信することで認証機能（本人確認等）を実現する。

③　認証書検証者、認証局間の手続きと交換する情報

A．認証書情報の公開

失効した認証書を公開する方法はＣＲＬ（認証失効リスト）やオンラインによる問合せなどの方法がある。以下に代表的な２通りの方法を示す。

- 認証書の有効性確認
  認証書検証者が認証局に対し相手企業の認証書情報を提示し現時点で認証書が失効されていないか問合せを行う。
- ＣＲＬの取得
  認証書検証者は認証局が一定期間毎に発行するＣＲＬを取得し該当する認証書がリストにあるかを確認する。

(2)　上記手続きと情報交換の処理形態およびワークフロー

上記手続きと情報交換を行うための処理形態としてそれぞれ以下に示す。

①　認証書の発行

被認証者が認証書の申請を行う場合、その方法として「オンラインによる申請」と「オフラインによる申請」が考えられる。

- オンラインによる申請
  被認証者が認証局に対しオンライン形態で申請を行う形式。認証局の申請フォームを画面に呼び出し、申請必要項目を埋め認証局に送信する。ただし、被認証者の正当性を保証する書類がある場合は、事前に受け渡されていなければならない。
- オフラインによる申請
  被認証者が認証局に対し郵送や出頭などをすることで申請を行う形式。申請に必要な書類及び、被認証者の正当性を保証するために必要な書類を同時に提出することができる。本人の出頭の場合、申請者が本人であることを証明する書類を提示する必要がある。

また、認証書の受渡し関してもその方法は「オンラインによる受渡」と「オフラインによる受渡」の２通りが考えられる。

- オンラインによる受渡
  必要に応じて、認証書の送付に際してセキュアな通信手段を講じる必要がある。
- オフラインによる受渡
  宅急便、書留郵便、配達証明等の受領確認ができるものを使用する。

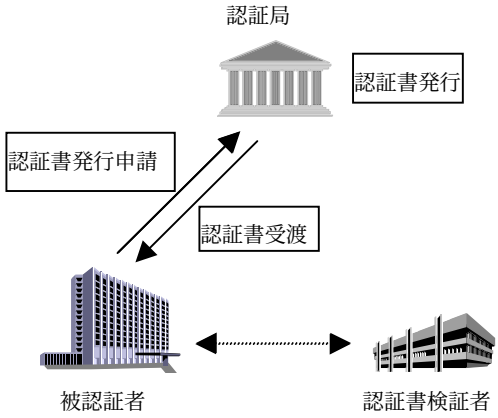

図 1-11 認証書の発行

② 認証書の更新

認証書の更新の形態は認証書の発行と同様に考えられるが、その内容については簡便化することも考えられる。

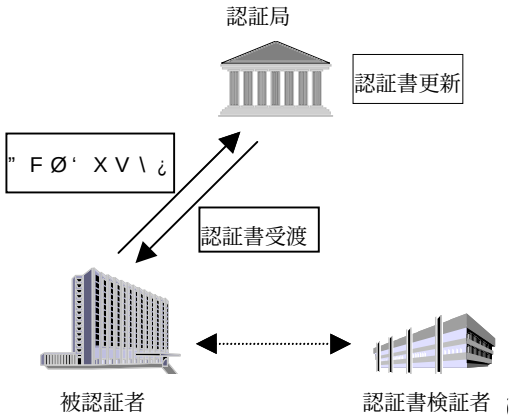

図 1-12認証書の更新

③　認証書の失効および一時失効

認証書の失効および一時失効の手続き形態は申請者によって異なる。被認証者が認証書の失効および一時失効を申請する場合、その方法は認証書の発行と同様に「オンラインによる失効申請／一時失効申請」と「オフラインによる失効申請／一時失効申請」が考えられる。

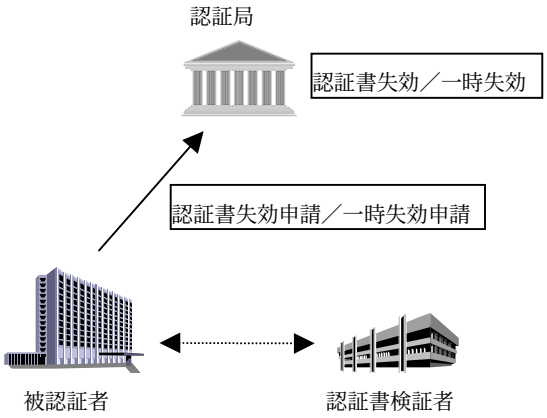

図 1-13被認証者からの申請による認証書の失効／一時失効

また、認証局による強制的な失効／一時失効を行う場合は、失効／一時失効処理の後、その結果について被認証者に通知を行う必要がありその方法は認証書の受渡と同様に「オンラインによる認証書の失効／一時失効通知」または「オフラインによる認証書の失効／一時失効通知」が考えられる。

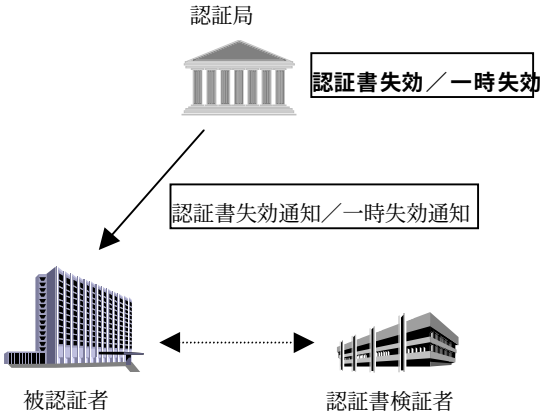

図 1-14認証局による強制的な失効／一時失効

④　認証書の送受信

認証書の送受信は取引きを行う企業間で取引き情報等を送受信するとき、オンラインで行う。

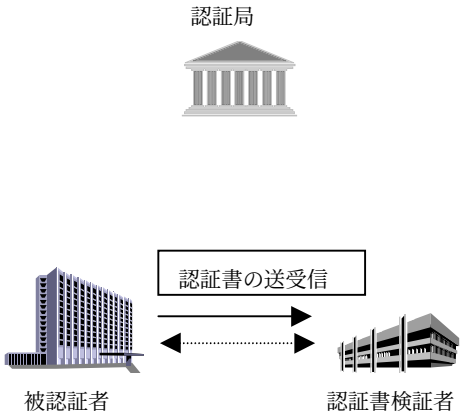

図 1-15認証書の送受信

⑤　認証書情報の公開

認証書情報の公開において認証書の有効性確認はオンラインで認証局に問合せを行う。認証局は認証書の状態（有効、失効、一時失効など）をオンラインで返す。

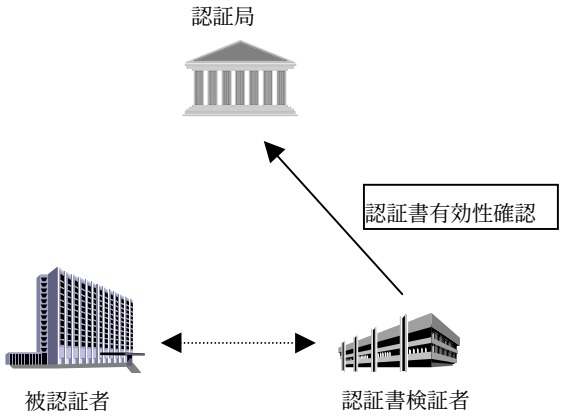

図 1-16認証書の有効性確認

また、CRL の取得においても被認証者は認証局に対しオンラインで CRL の取得を行う。

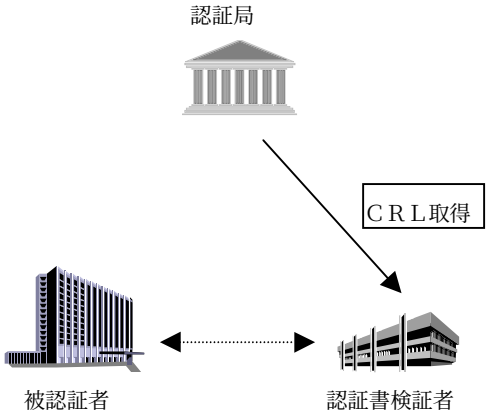

図 1-17CRL の取得

1.3. 公的認証との関連

本節では、公的機関と民間企業、民間企業間の電子商取引における、公的機関の行う認証機能の位置づけ、認証のベースとなる資格要件との関係を示す。

なお、ここでの“公的”の意味は“公的な機関が行う”ということである。

1.3.1. 適用する認証の取引きにおける位置づけ

(1) 取引きにおける公的資格・要件の必要性

実世界での公的機関と民間企業との取引きにおいては、公的機関による民間企業に対する取引資格の審査がある等で、取引きの実施に一定の資格要件が要求されることがある。従って、公的機関と民間企業との電子商取引において、取引審査との関連で公的機関が発行する認証書の使用が要求される事がありうる。

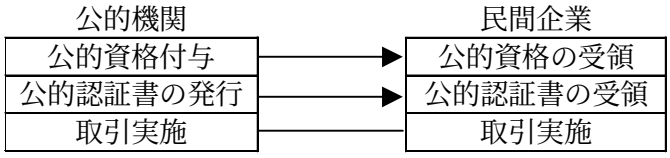

図 1-18資格付与と認証発行が一体となった場合

勿論、認証書の発行と公的資格の審査・付与の機能を分離し、認証書による相手確認後に何らかの方法で相手の資格条件を確認するという方式もありうる。

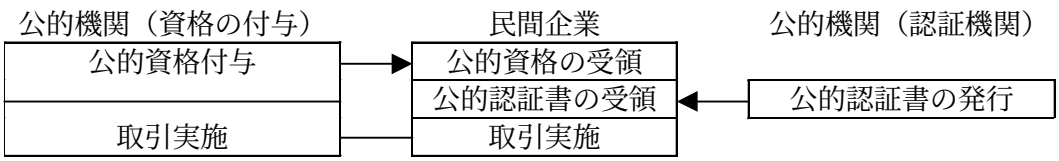

図 1-19資格付与と認証発行が分離した場合

一方民間企業間の取引きでは、基本的には個々の取引当事者間の合意によって成立するので、そこに公的な機関が介在する必然性は無いと考えられる。しかし、取引きの信頼性を高めるため等の目的で、取引参加者に一定の公的な資格要件を要求することは、現実世界の取引きにおいてはある。従って、民間企業間の電子商取引においても、これは当てはまると考えられる。

公的な認証を利用する可能性として考えられるのは、以下の様なケースである。

- 取引きの実施に当たって公的な資格要件が必須な場合
- 取引きを安全・確実に実現するため、取引当事者が相手に公的資格要件を要求する場合

通常は“信用”によって、これらの資格検証は省略されるが、電子商取引においてはオープンな取引形態が増加することにより、まだ“信用”形成されない相手・段階でも取引きを実施する事が想定されるので、取引きの信頼性を補強する目的で公的認証を利用するものである。勿論、民間認証局による信頼性の補強も当然あり、利用者の判断等で公的認証機関を利用するか、民間認証機関を利用するかは決まる。

(2)　必要な公的資格・要件と認証の関係

認証書の発行において公的な資格要件が必要とされる場合は、認証における審査と認証書の発行主体が、公的な資格要件の付与者である、という関係になる。これはＸ．５０９認証書を用いて相手確認した取引当事者が、相手が、当該公的機関の付与する公的な資格要件を、認証書発行時点で所持していたことの確認を、相手確認と同時に行う事になる。資格要件はダイナミックに変更しうるので（資格要件の喪失等）、認証書による本人・資格要件確認だけでは、資格要件の確認は不十分である。従って、公的機関は資格要件付与認証に関する情報サービスの提供等を利用した確認が必要になる。このため、認証と資格要件の検証をプロセスを分けて実行する方式が、効率的な場合もありうる。この場合は、公的資格付与機能と公的認証機能は別の機関が実施することになる。

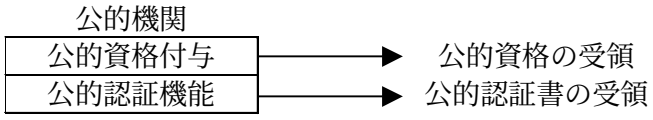

図 1-20資格付与と認証発行が一体となった場合

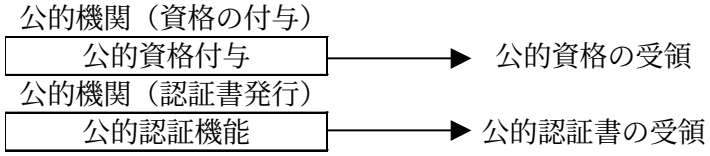

図 1-21資格付与と認証発行が分離した場合

第2章　企業間取引における公証適用の考え方

本章では、企業間取引において公証機能の利用を検討する際に参考とすべき公証モデル、公証ポリシー、公証のワークフローに関する一つの考え方を示すことにより、企業間取引における公証適用の考え方のガイドラインを目指すものである。なお、公証適用の前提として第１章に記載する認証局を利用した企業認証の適用が成されているものとする。

2.1.　公証モデル

公証モデルを検討する前提として、公証の定義をしておく必要がある。ＥＣＯＭが作成した「電子公証システムガイドライン　Ｖ．１.０」において電子公証の定義を与えている。それによると電子公証の対象範囲を非常に広くとらえて公証を定義しているため、ここでは更に「企業認証・公証」に限定した公証の定義を行う。

＜「電子公証システムガイドライン　Ｖ．１.０」による公証の定義＞

ネットワーク上の商取引等における電子的交流の安全･信頼性を確保する仕組みにおいて、その一構成要素として位置づける

＜企業認証・公証における公証の定義＞

企業間電子商取引における取引当事者と第三者との間で、電子商取引に関するなんらかの紛争が発生した場合、その紛争処理を容易にするため、当該取引行為および取引当事者に係わる情報を、改竄できないよう保存する等の機能またはサービスを「公証」と呼ぶ。

（注）ここで言う「公証」とは、「公が証する」という意味ではなく、「公に証する」という意味で用いている。

2.1.1.　　公証モデルの検討範囲

本書で検討する企業公証モデルの範囲を明確にするため、まず公証機能を適用すべきビジネスモデルの観点から次の２つに分類する。

(1)　　契約型モデル

商取引などの企業間交流を目的とするクローズドなグループを構成する企業群において、紛争発生時の事実確認手段として公証機能を利用することを、当該グループへの参加条件とする場合のモデル。公証機能の実現方法として、取引当事者が公証機能を具備する場合と、第三者の提供する公証機能を利用する場合とが考えられる。公証機能を提供する機関は当該グループ内で予め約款等により、その利用と効力を明らかにしておく必要がある。

(2)　　公募型モデル

取引所あるいは公募の主催企業と、不特定の応募企業との、事前の契約関係を前提としない取引形態において、取引当事者または第三者からの事実確認要求に対応するために、公証機能を用いる場合のモデル。公証機能の実現方法として、取引当事者が公証機能を具備する場合と、第三者の提供する公証機能を利用する場合とが考えられる。

これらのモデルにおける公証機能としては、法的効力を有する公的機関または公的機関から承認された機関が提供するサービスを利用する場合も考えられるが、それらの公的な公証サービスに関しては、本書の検討対象外とする。

2.1.2.　公証の対象と公証の機能

公証で取り扱うべき対象と、公証に必要であると考えられる機能の代表的なものとして、以下のものを挙げることができる。

(1)　公証の対象

公証では、以下の各対象に対する各種の証明を行う。

①　企業間取引を実行した当事者に関する情報

取引きの当事者に関する所定の情報を証明する。

例えば次のような情報を含む。

- 取引実行企業を識別した事実
- 取引実行担当者を識別した事実
- 取引実行企業または担当者が有資格者であったことの事実

②　企業間取引行為に関する情報

取引きを構成または規定する情報を表現したデジタルデータを証明の対象とする。

例えば次のような情報を含む。

- 注文情報の内容（品名、数量、金額、等）
- 注文情報発信時刻
- 注文情報の相手企業への到達確認

(2)　公証の機能

公証機能として、(1)項で示した各々の対象に関する以下の証明機能を例として挙げる。

①　取引データの発行者の証明

企業間取引に使用されたデジタルデータの発行者が誰かということを証明する。発行者としては、企業代表者、取引担当者など、種々の場合が想定されるが、それら公証の対象となる者は認証の対象であることが前提となる。

なお、企業間取引におけるデジタルデータの発行者であることの証明は、そのデジタルデータの所有権、著作権を有することを証明するものではない。（公証の対象外）

②　取引データの存在証明

企業間取引に使用されたデジタルデータが存在した時刻の証明、そのデジタルデータを特定できる情報を記録しておくことにより取引データ本体の存在の証明が可能となる。取引データとしては、企業間取引に使用される各種のドキュメント等が含まれる。

企業が取引データ受信時に確認メッセージを返送する機能等を併用することにより、取引データの到達確認の証明が可能となる。

③　取引データの真正性の証明

企業間取引に使用されたデジタルデータの内容とそれが改竄されていないことを証明する。取引データの保管機能を備えることにより取引データの内容そのものの証明が可能となる。

④　取引プロセス、取引データ処理プロセスの証明

企業間取引のプロセスや取引データ処理のプロセスを記述する情報を記録し、その情報を真正性の維持できる条件下に保管することにより、取引プロセス、取引データ処理プロセスを証明する。

2.1.3.　公証機関によるモデルの分類

企業公証のモデルをその提供者である公証機関の観点から分類する。

公証機関とは、企業間取引の当事者に対して公証機能を提供する機関を指す。

公証利用者とは、企業間取引の当事者であり、公証機関が提供する公証機能を利用する企業を指す。取引相手または第三者からの取引事実等に関する証明要求に対して、公証機能を利用する。

企業公証を提供する公証機関の数に着目して以下に公証モデルを分類する。

(1)　単一公証機関モデル

公証利用者の属するグループでは、ただ１つの公証機関が有効であるようなモデル。

このモデルでは、公証機関が１つだけ存在する。１つの利用すべき公証機関、公証機能を利用するための条件等を当該グループの約款等で規定し、グループ内の各企業は規定された公証機関の提供する公証機能を利用する。このモデルは、特定企業とその資材調達先企業群など、予め取引条件や責任の範囲と分界点などに関して契約で合意した関係にある企業群への適用に適したモデルである。ビジネスモデルの契約型モデルでは一般的に単一公証機関モデルが適用できる。

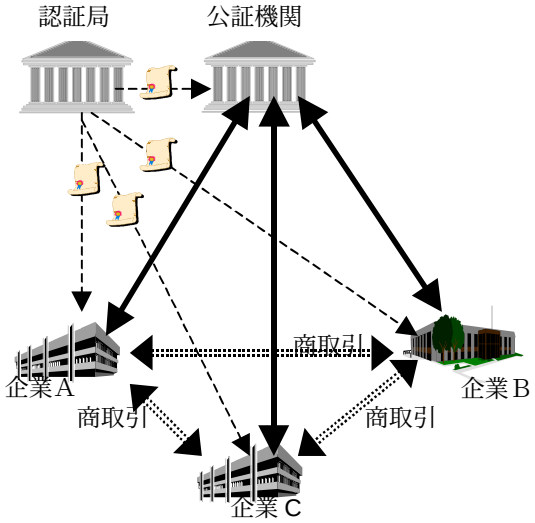

図 2-1 単一公証機関モデル

(2)　複数公証機関モデル

公証利用者の属するグループでは、２つ以上の公証機関が有効であるようなモデル。

このモデルでは、公証機関が複数存在し、利用者はいずれの公証機関を利用してもよい。

このモデルは、公開入札や競売などの取引形態への適用に適したモデルである。取引の公平性、客観性の確保に関して公証機能を適用することが考えられる。ビジネスモデルの公募型モデルでは一般的に複数公証機関モデルが適用できる。

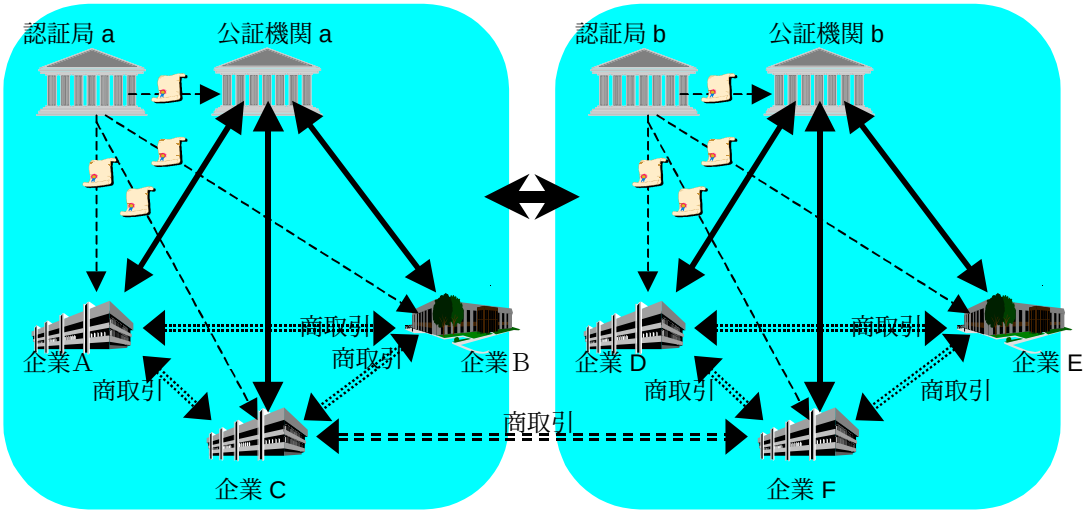

図 2-2 複数公証機関モデル

2.2.　公証ポリシーの策定

公証の適用にあたり、まずその目的と目標を明確にしておくべきである。その上で公証機能に対する要件と実現方法、運用などについて、対象システムのライフサイクル全体にわたり、規定するべきである。このような基本的な考え方を「公証ポリシー」として策定すべきであると考える。しかし、企業間電子商取引における公証機能および適用方法などは現状ではまだ確立されておらず、従って公証ポリシーの策定例は知られていない。このため本書では、公証ポリシーの必要性と１つの考え方を述べるにとどめる。今後公証機能の効力や関連する法律、制度などの環境条件の整備の過程で、公証ポリシーに対する議論が深められるものと考える。

2.2.1.　公証ポリシーとは

公証ポリシーとは、同一の公証機能を適用することを合意した企業群（これを公証ドメインと呼ぶ）において、公証機能により担保すべき安全性・信頼性に対する基本的考え方およびその実現方法等を規定するものである。また、公証ポリシーでは、当該公証ドメインにおいて適用する公証機能の具体的な実現方法、すなわちどのような公証機関および公証機能を利用するべきか、各々の企業が備えるべき公証機能の範囲と運用方針、等を規定する。

公証ポリシーにおいて規定すべき事項として、以下の項目が考えられる。

- はじめに
- 一般条項
- 目的
- 前提となるセキュリティポリシー、認証ポリシー
- 公証要件

- 業務上の要件
- 運用上の要件
- コンティンジェンシープラン

2.2.2. 公証ポリシーの形成過程

我が国では、従来企業間電子商取引（ＥＤＩ）を開始しようとする企業は、特定の取引先企業との間で取引基本契約を締結するのが一般的である。この取引基本契約において、取引上の責任範囲とその分界点について規定する。また、特定の企業群において相互にＥＤＩを行う場合には、ＶＡＮを利用する例が多く、そのＶＡＮ運営者が策定した約款や利用規程において、ＶＡＮ運営者と接続企業との間の責任範囲とその分界点を規定している。

しかし、従来のＶＡＮを用いたＥＤＩに比べて、インターネットを用いた電子商取引においては、考慮すべき脅威の増大、取引当事者間での責任における分界点のあいまいさの増大などが生じる可能性がある。電子商取引におけるこの種の問題に対しては、電子的な公証機能の利用が１つの対策となり得る。

このように公証機能を利用する場合には、その適用用途や適用範囲、適用機能などに関して、取引当事者間で合意がなされている必要がある。また、取引参加の可否を判断しようとする企業が取引に参加した場合のリスクを客観的に判断することのできる情報の開示が必要となる。

これらの要件に応えるものとして、公証ポリシーの制定と開示が求められることになるものと考えられる。

公証ポリシーを持たない商取引のグループ、すなわち公証ドメインに対しては、取引の安全性に対する不安から、新たに取引参加を希望する企業が現れない可能性があるばかりでなく、既に参加している企業間においても紛争発生時に適切な処置ができないことから、その公証ドメインは淘汰されるであろう。

公証ポリシーの策定から維持に至るプロセスをモデル化すると、表２－１のようになる。

表 2-1 公証ポリシー策定の過程

#	プロセス	内容	担当
1	基本ビジネス検討	電子商取引における公証の必要性と適用に関する基本方針の検討	ビジネス責任者
2	公証ポリシー制定主体の確定	公証ポリシー制定主体の決定	ビジネス責任者
3	認証ポリシー策定	準拠している認証ポリシーの参照	ビジネス責任者
4	公証要件の定義	公証適用対象と範囲、必要機能の定義	ビジネス責任者 公証ポリシー制定主体
5	公証構造の決定	当該公証ドメインの定義、公証提供者、公証利用者の定義、義務と責任範囲の規定	公証ポリシー制定主体
6	公証ポリシー策定	公証ポリシーの検討、明文化	公証ポリシー制定主体
7	基本ビジネス計画との適合性検討	取引基本契約などとの整合性の確認、フィードバック	ビジネス責任者 公証ポリシー制定主体
8	参加者、利用者への公開	参加者（企業）、利用者（企業）に対する公証ポリシーの公開	公証ポリシー制定主体
9	ビジネスの実施	実ビジネスへの公証機能の適用	ビジネス責任者 公証ポリシー制定主体
１０	公証ポリシー改訂	ビジネスを実施した結果による、ポリシーへのフィードバック	公証ポリシー制定主体

2.3. 公証のワークフロー

公証のワークフローを検討するに当たり、公証のワークフローをまず取引データの経路により２つの形態に分類する。それらの各々の形態毎に、公証データの登録と証明の２つのワークフローについて図示する。

2.3.1. 取引データの経路が公証機関を経由する形態

公証利用者が公証の対象とすべき取引データを、公証機関を経由して取引相手に送信する形態である。公証機関は公証利用者から送付された取引データに対して公証サービスに応じた処理を施し、それを取引相手企業に送信する。公証機関において取引データを保存する場合もある。また、公証の対象としない取引データも全て公証機関を経由させる形態と経由させない形態とが考えられる。

(1) 公証データの登録

公証利用者は公証機関を経由して取引相手企業と送受信する取引データのうち、公証の対象とするものを公証機関に指示する。公証機関は公証利用者から指示された取引データに対して公証データとしての登録処理を行う。具体的な処理は公証機能に依存するが、一般的に公証に必要となる情報の付加、公証機関の署名などをおこなうものと考えられる。公証機関は公証データの登録が済んだ取引データを所定の企業（公証利用者またはその取引先企業）に送信するとともに、公証利用者に公証済みデータとして送信する。

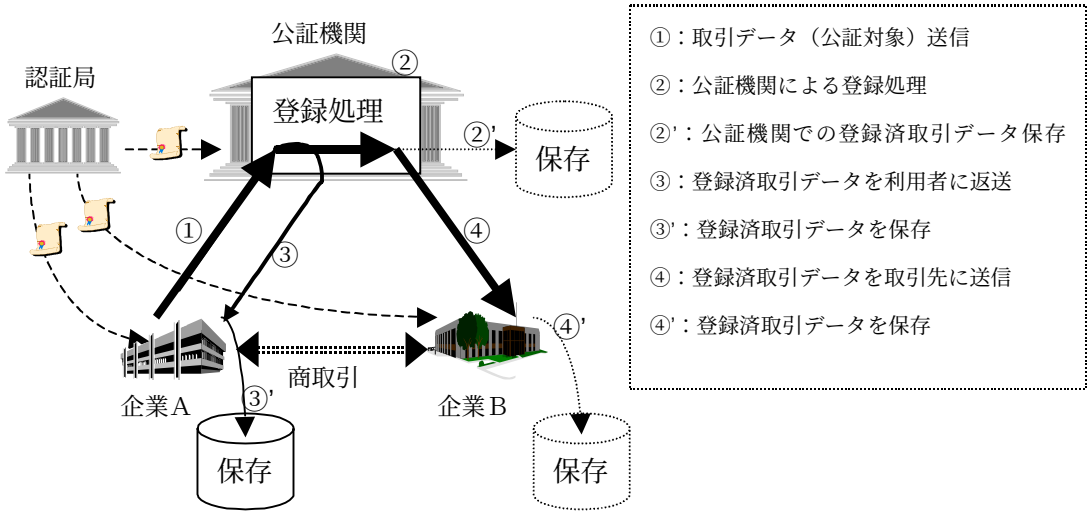

図 2-3公証機関経由による公証データの登録

(2)　証明

公証利用者と他の企業との間で紛争が発生した場合に、公証利用者は公証機関に登録処理を行い保管しておいた取引データ等を取り出し、紛争の相手に提示する。提示を受けた企業は、取引内容の確認や取引の妥当性を検証し、取引当事者あるいは公証機関に疑義を持つならば、認証局を利用し、それらの証明書の確認を行うことができる。

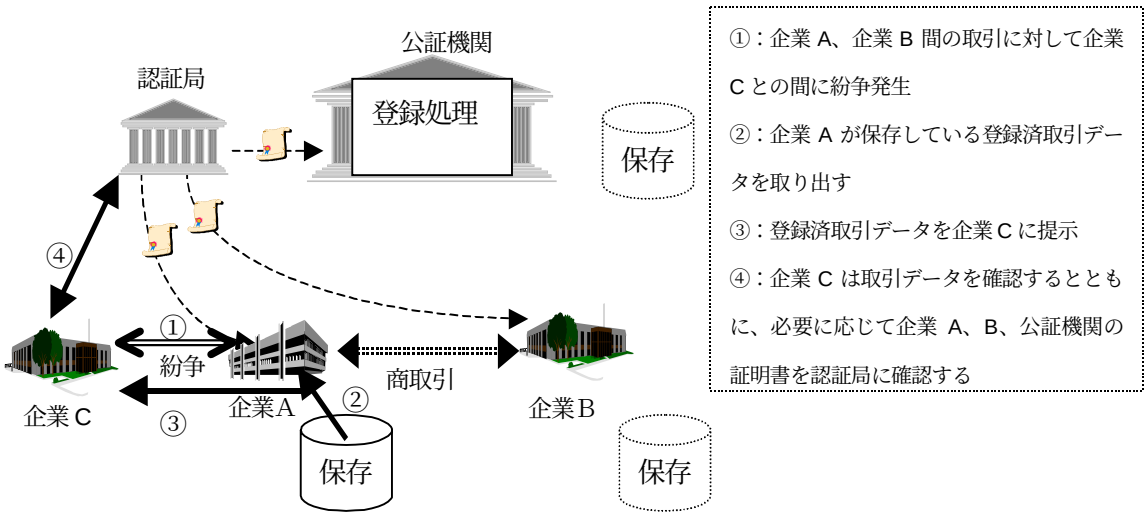

図 2-4証明

2.3.2.　取引データの経路が公証機関を経由しない形態

公証の利用者が公証の対象とすべき取引データを、取引相手への送信に先立ち、公証機関に送信する。公証機関は送付された取引データに対して公証サービスに応じた処理を施し、それを利用者に返送する。その際に公証機関で取引データを保存する場合もある。利用者は公証機関から返送された登録済みの取引データを、公証機関を経由しない経路で取引先に送

信する。

(1)　公証データの登録

公証利用者は取引相手企業と送受信する取引データのうち、公証の対象とするものを、公証機関に提示し、登録を依頼する。公証機関は公証利用者から提示のあった取引データに対して公証データとしての登録処理を行う。具体的な処理は公証機能に依存するが、一般的に公証に必要となる情報の付加、公証機関の署名などをおこなうものと考えられる。公証機関は公証データの登録が済んだ取引データを公証利用者に返す。公証利用者は、登録の住んだ取引データを必要に応じて取引先企業に送信するか、あるいは取引先企業からの受信データとしての処理を行う。

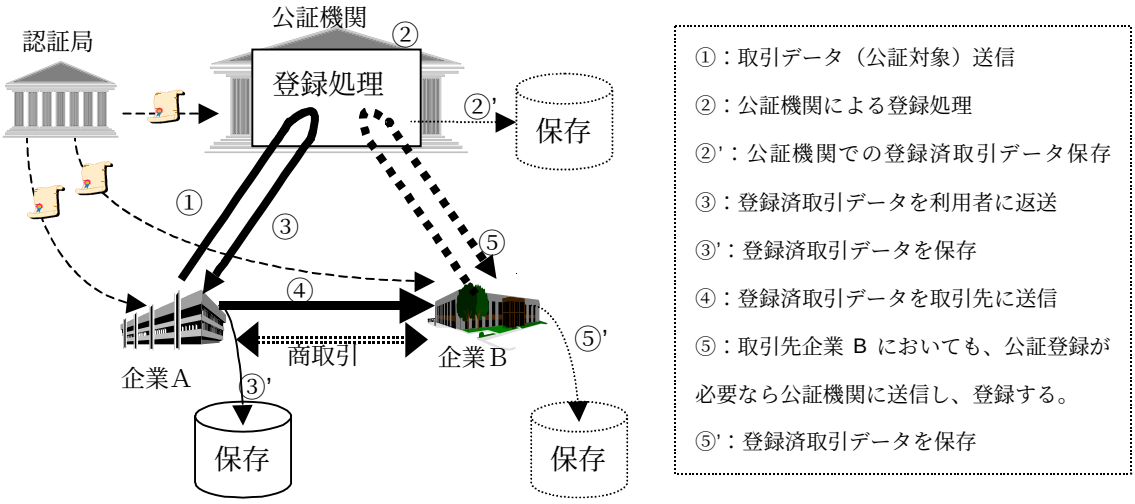

図 2-5公証機関を経由しない公証データの登録

(2)　証明

２．３．１(2)項と同様のワークフローとなるものと考えられるため、記載を省略する。

2.4.　公的公証との関連

本章では、公的機関と民間企業、民間企業間の電子商取引における、公的機関の行う公証の位置づけ、公証機能のベースとなる資格要件との関係を示す。

なお、ここでの“公的”の意味は“公的な機関が行う”ということである。

2.4.1.　適用する公証の取引きにおける位置づけ

(1)　取引きにおける公的資格・要件の必要性

実世界の公的機関と民間企業間の取引きでは、取引事実の確認は公的機関側の証跡を信用することで足りると考えられる。電子商取引では電子データの交換による取引きとなり、実世界とは環境が異なるが、やはりこの取引きの証明力を高めるため、公的公証機関による電子的な公証が必要になる場合があると想定される。

一方民間企業間の取引きでは、基本的には個々の取引当事者間の合意によって成立するので、そこに公的な機関が介在する必然性は無いと考えられる。しかし、取引きの信頼性を高めるため等の目的で、取引参加者が公的な資格要件有する公的公証機関を利用することは、現実世界の取引きにおいてはある。従って、民間企業間の電子商取引においても、これは当

てはまると考えられる。

公的な公証を利用する可能性として考えられるのは、以下の様なケースである。

- 取引きにあたり、取引きの事実関係（時刻等）に公的機関による証明が必要な場合
- 取引当事者以外の不特定多数の外部から、取引内容に関しての証跡が求められうる場合
- 取引証跡に法律的な有効性を付与する必要がある場合

公的な公証を要するのは法的に要求される場合を除いて、上記のように取引当事者間だけに通用する公証では、証明力不足と推定される場合、これを補強するため取引当事者の判断で利用する場合である。

(2)　必要な公的資格・要件と公証の関係

公的な公証においては、公証行為を行う機関が公的資格を所有するという関係になる。これは取引証明によって証明される事柄が、その取引内容の事実関係となり、それを証明するのは取引当事者と直接的な利害関係が無くかつ、その公証行為に必要な証明能力があると取引当事者及び第三者が認めることが必要であり、それを認めるためには公的な資格要件を満たすことが前提となるためである。

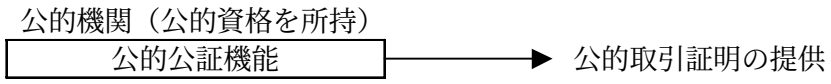

図 2-6公的公証と資格資格の関係

付録

A 参考文献

(1) 認証局運用ガイドライン（V1.0）、電子商取引実証推進協議会 認証局検討ＷＧ、1998.4
(2) 本人認証技術検討ＷＧ報告書、電子商取引実証推進協議会 本人認証技術検討ＷＧ、1998.3
(3) 電子公証システムガイドライン（V1.0）、電子商取引実証推進協議会 電子公証ＷＧ、1998.3
(4) 電子取引法制に関する研究会（精度関係小委員会）報告書、法務省、1998.3
(5) 電子商取引環境整備研究会 中間論点整理、通産省、1997.11
(6) CARAT Guidelines V.1.0, National Automated Clearing House Association, 1998.9.21
(7) R. Housley, W. Ford, W. Polk, D. Solo, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, IETF PKIX Working Group, 1999.1
ftp://ftp.isi.edu/in-notes/rfc2459.txt
(8) S. Farrell, C. Adams, Internet X.509 Public Key Infrastructure Certificate Management Protocols, IETF PKIX Working Group, 1999.3
ftp://ftp.isi.edu/in-notes/rfc2510.txt
(9) S. Chokhani, W. Ford, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, IETF PKIX Working Group, 1999.3
ftp://ftp.isi.edu/in-notes/rfc2527.txt
(10) C. Adams, R. Zuccherato, Internet X.509 Public Key Infrastructure Data Certification Server Protocols, IETF PKIX Working Group, 1998.9.23
http://www.ietf.org/internet-drafts/draft-ietf-pkix-time-stamp-00.txt
(11) M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, 1998.9
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ocsp-07.txt

B 検討メンバー

ECOM

米倉 昭利　　電子商取引実証推進協議会 主席研究員
菅　知之　　電子商取引実証推進協議会 主席研究員
加藤 寛之　　電子商取引実証推進協議会 主席研究員

リーダー・サブリーダー

鍛冶 俊彦　富士通株式会社第二ｼｽﾃﾑ事業部 EC ソリューション推進室 担当課長
光永 聖　株式会社日立製作所情報ｼｽﾃﾑ事業部 金融ﾋﾞｯｸﾞﾊﾞﾝ推進本部 商品開発第二ｾﾝﾀ/IC ｶｰﾄﾞｼｽﾃﾑﾋﾞｼﾞﾈｽ推進ｾﾝﾀ ｾﾝﾀ長
黒岩 博孝　日本電気株式会社 EC 推進本部ｼｽﾃﾑ部 ﾏﾈｰｼﾞｬｰ

メンバー

鈴木　晃　株式式会社アニモ 開発推進部 部長
家木 俊温　株式会社NTTﾃﾞｰﾀ 技術開発本部 ﾏﾙﾁﾒﾃﾞｨｱ技術ｾﾝﾀｰ 担当課長
田吹 隆明　株式会社ｷｬﾃﾞｨｯｸｽ 社長付 ｼﾆｱﾘｰﾀﾞｰ
深谷 清之　財団法人金融情報ｼｽﾃﾑｾﾝﾀｰ 業務調査部 業務調査第二課 課長
保倉　豊　ｸﾞﾛｰﾊﾞﾙﾌﾚﾝﾄﾞｼｯﾌﾟ株式会社　代表取締役社長
北田 容一　株式会社三和銀行 決済業務部 部長代理
宮下 善和　神鋼電機株式会社 開発本部商品開発部
藤本　武　綜合警備保障株式会社 技術部 情報通信課
吉田 耕造　株式会社大和総研 ｲﾝﾀｰﾈｯﾄ事業室 課長
星野　理　株式会社帝国ﾃﾞｰﾀﾊﾞﾝｸ 企画部企画課
高橋 和博　東電ｿﾌﾄｳｪｱ株式会社 CALS/EC技術部 主任
中道 一人　日本ｱｲ･ﾋﾞｰ･ｴﾑ株式会社 e-ビジネス事業開発 市場開発 主任
有本 忠男　財団法人日本品質保証機構 南関東試験センター 事業推進第一課 課長
出口 太郎　株式会社富士総合研究所 研究開発第２部 研究員
河瀬 恭一　松下電器産業株式会社 公共ｼｽﾃﾑ営業本部ｼｽﾃﾑ推進部 ｼｽﾃﾑ二課 主任技師
大谷 彰宏　三菱電機株式会社 流通･ｻｰﾋﾞｽ･通信ｼｽﾃﾑ部 EC事業推進G 専任
須田　章　安田火災海上保険株式会社 事務企画部 企画ｸﾞﾙｰﾌﾟ 副長

平成１１年３月発行
発行：電子商取引実証推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel 03-5531-0061
E-mail info@ecom.or.jp